UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,158	12/02/2003	Simon Robert Walmsley	PEA24US	6703

24011   7590   09/26/2007
SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER
NALVEN, ANDREW L

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
09/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/727,158	WALMSLEY, SIMON ROBERT
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>17 September 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-18 and 20</u> is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-18 and 20</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on <u>02 December 2003</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☒ All   b)☐ Some * c)☐ None of:

         1.☒ Certified copies of the priority documents have been received.

         2.☐ Certified copies of the priority documents have been received in Application No. _____.

         3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-18 and 20 are pending.

Response to Arguments

2.   Applicant's arguments regarding the rejections under 35 USC § 112 are

persuasive.

3.   Applicant's remaining arguments filed 17 September 2007 have been fully

considered but they are not persuasive.

4.   Applicant has argued in pages 1-2 that the Mi reference fails to teach the

identifiers for the series are determined in such a way that knowing the identifier of one

of the integrated circuits does not improve the ability of an attacker to determine the

identifier of any of the other integrated circuits. Examiner respectfully disagrees. Mi's

identifier (processor number) is statistically unique. An attacker knowing a statistically

unique number would not assist the attacker in determining the identifier of any of the

other integrated circuits. Applicant has provided no basis for the assertion that knowing

a statistically unique would aid an attacker. Further, the limitation in question is not a

method step nor does it provide any structural elements that distinguish it from the prior

art. Language that suggests or makes optional but does not require steps to be

performed or does not limit a claim to a particular structure does not limit the scope of a

claim or claim limitation (MPEP 2106). Because the cited limitation fails to provide any

method steps or structural elements it does not effect the scope of the claim and its

effect upon the scope of the claim will be limited. As a result, Examiner maintains the

rejection of claim 1 in view of the Mi reference.

5.   The rejections appearing below are identical to those presented in the prior office

action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6.   **Claims 1-3, 5, and 7-17 are rejected under 35 U.S.C. 102(e)** as being

anticipated by Mi et al US PGPub 2002/0116616.

7.   **With regards to claim 1**, Mi teaches determining a method of manufacturing a

series of integrated circuits having related functionality, the method including the steps

of determining an identifier (Mi, paragraph 0021, processor number), permanently

storing the identifier on one of the integrated circuits (Mi, paragraph 0021, stored in a

constant ROM or processor ID register), repeated steps (a) and (b) for each integrated

circuit in the series (Mi, paragraph 0021, more than one device has processor number),

wherein the identifiers for the series are determined in such a way that knowing the

identifier of one of the integrated circuits does not improve the ability of an attacker to

determine the identifier of any of the other integrated circuits (Mi, paragraph 0021,

statistically unique for a given processor).

8.   **With regards to claim 2**, Mi teaches the identifier for each integrated circuit is

determined using a stochastic mechanism thereby rending highly improbably that

replication of some or all of the series of identifiers stored on the series of the integrated

circuits (Mi, paragraph 0021, statistically unique).

9.   **With regards to claim 3**, Mi teaches each of the integrated circuits incorporates

an identifier determined and stored in accordance with claim 1 (Mi, paragraph 0021,

more than one device has processor number).

10.   **With regards to claim 5**, Mi teaches the integrated circuit operable in a first and

second mode (Mi, paragraph 0042, authorized or unauthorized state), wherein in the

first mode, supervisor code can access the identifier (Mi, paragraphs 0042-0043,

applets that are verified and authorized can access processor number) and in the

second mode, user code cannot access the identifier (Mi, paragraphs 0042-0043,

applets that are not verified and not authorized cannot access processor number).

11.   **With regards to claim 7**, Mi teaches the identifier mapped into a key K (Mi,

paragraph 0024, identifier mapped into XOR result of identifier-211 and secret key).

12.   **With regards to claim 8**, Mi teaches that K is the identifier (Mi, paragraph 0021,

processor number).

13.   **With regards to claim 9**, Mi teaches K is created by applying a hash function or one-way function to the identifier (Mi, paragraph 0024, identifier is hashed using SHA-1 or MD5).

14.   **With regards to claim 10**, Mi teaches the integrated circuit configured to produce and output a message from the integrated circuit (Mi, paragraph 0030, client computer sends return value to server) the message including a result of encrypting K (Mi, paragraph 0030, paragraph 0031, paragraph 0024, second XOR on intermediate value-K using session identifier).

15.   **With regards to claim 11**, Mi teaches injecting a key into a target integrated circuit (Mi, paragraph 0030, server receives return value) comprising the step of receiving the message generated by the first integrated circuit of claim 10, and transferring a second key into the target integrated circuit (Mi, paragraph 0030, server receives return value), the second key being based on K (Mi, paragraph 0024, second XOR on intermediate value-K using session identifier).

16.   **With regards to claim 12**, Mi teaches generating the second key by manipulating K with a function (Mi, paragraph 0024, K manipulated using second XOR function).

17.   **With regards to claim 13**, Mi teaches the function uses K and a code associated with the target integrated circuit as operands (Mi, paragraph 0024, function uses K and session identifier associated with session between client and server).

18.   **With regards to claim 14,** Mi teaches that the code is a code that is relatively unique to the target integrated circuit (Mi, paragraph 0023).

19.   **With regards to claim 15,** Mi teaches K and the second key enabling secure communication between the first integrated circuit and the target integrated circuit (Mi, paragraph 0031, K and return value-second key are used by server to determine if access is permitted, paragraph 0036).

20.   **With regards to claim 16**, Mi teaches the second integrated circuit configured to communicate securely with a third integrated circuit (Mi, paragraphs 0052-0054, web server communicates with those seeking to participate in a teleconference), thereby enabling it to act as an intermediary between the first integrated circuit and the third integrated circuit (Mi, paragraphs 0052-0054, web server acts as intermediary between members of the teleconference) allowing secure communication there between (Mi, paragraph 0055).

21.   **With regards to claim 17**, Mi teaches the first and third integrated circuits do not share a key for use in the secure communication (Mi, paragraph 0061, web server acts as a gatekeeper).

Claim Rejections - 35 USC § 103

        The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

22.   **Claims 4, 18, and 20 are rejected under 35 U.S.C. 103(a)** as being

unpatentable over Mi et al US PGPub 2002/0116616 in view of Debry US Patent No.

6,314,521.

23.   **With regards to claim 4**, Mi fails to teach the integrated circuits being printer

controllers. However, Debry teaches each integrated circuit being a printer controller

(Debry, column 8 lines 18-29, unique encryption key embedded in each manufactured

printer). At the time the invention was made, it would have been obvious to a person of

ordinary skill in the art to utilize Debry's method of placing unique identifiers within

printer controllers because it offers the advantage of allowing a printer to be able to

prove to a sender that it is the actual printer device that the printer purports to be

(Debry, column 5 lines 65-67, column 6 lines 4-11).

24.   **With regards to claim 18**, Mi teaches a first integrated circuit configured to

perform an authenticated read of a third integrated circuit by securely communicating

via the second integrated circuit (Mi, paragraph 0061, server forwards identifiers), but

fails to teach the first integrated circuit being a print controller. However, Debry teaches

an integrated circuit being a printer controller (Debry, column 8 lines 18-29, unique

encryption key embedded in each manufactured printer). At the time the invention was

made, it would have been obvious to a person of ordinary skill in the art to utilize

Debry's method of placing unique identifiers within printer controllers because it offers

the advantage of allowing a printer to be able to prove to a sender that it is the actual

printer device that the printer purports to be (Debry, column 5 lines 65-67, column 6

lines 4-11).

25.   **With regards to claim 20**, Mi as modified teaches the authenticated read

relating to monitoring or updating usage of a resource (Debry, column 8 lines 18-30 and

53-56, printer is updated with digital certificate).

26.   **Claim 6 is rejected under 35 U.S.C. 103(a)** as being unpatentable over Mi et al

US PGPub 2002/0116616 in view of Collins et al US Patent No. 7,055,029.

27.   **With regards to claim 6,** Mi fails to teach the supervisor mode being available to

a program upon verification of that program by a boot program of the integrated circuit.

However, Collins teaches teach the supervisor mode being available to a program upon

verification of that program by a boot program of the integrated circuit (Collins, column 5

lines 7-15, column 9 line 65 – column 10 line 17, control of processor is transferred to

black-boot program upon verification). At the time the invention was made, it would

have been obvious to a person of ordinary skill in the art to utilize Collin's method of

verifying program using a boot program because it offers the advantage of ensuring the

security of the computer system itself and of all processes handled by the computer

system (Collins, column 2 lines 40-49).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

The prior art made of record and not relied upon is considered pertinent to

applicant's disclosure.

28.   Cordery et al US Patent No. 6,064,989 discloses a method of synchronization of

cryptographic keys between two modules.

29.   DeBry US Patent No. 6,385,728 discloses a method for providing will call

certificates for guaranteeing authorization for a printer to retrieve a file directly from a file

server.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Andrew L. Nalven whose telephone number is 571 272

3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate

Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Andrew Nalven

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER